使用 GetStartupInfo 检查自己是否被"调试"（转自看雪论坛）

转载

anppcw1784 于 2012-07-13 14:49:00 发布 92 收藏
文章标签： php 操作系统
原文链接：http://www.cnblogs.com/02xiaoma/archive/2012/07/13/2590227.html

原文地址：http://bbs.pediy.com/showthread.php?t=31447

在使用 CreateProcess 创建进程时,需要传递
STARTUPINFO 的结构的指针,
而常常我们并不会一个一个设置其结构的值,
连把其他不用的值清0都会忽略,
而 ollydbg 也这样做了,
我们可以使用 GetStartupInfo 检查启动信息,
如果很多值为"不可理解"的,那么就说明自己不是由 explorer 来创建的.(explorer.exe 使用 shell32 中 ShellExecute 的来运行程序, ShellExecute 会清不用的值)

还有一点 ollydbg 会向 STARTUPINFO 中的 dwFlags 设置 STARTF_FORCEOFFFEEDBACK,而 explorer 不会

```
1
2 //ex
3
4 #include <windows.h>
5 #include <stdio.h>
6
7 #pragma comment(linker, "/subsystem:windows /entry:main")
8
9 int main()
10 {
11   STARTUPINFO si;
12
13   GetStartupInfo(&si);
14
15   if (
16     (si.dwX != 0) ||
17     (si.dwY != 0) ||
18     (si.dwXCountChars != 0) ||
19     (si.dwYCountChars != 0) ||
20     (si.dwFillAttribute != 0) ||
21     (si.dwXSize != 0) ||
22     (si.dwYSize != 0) ||
23     (si.dwFlags & STARTF_FORCEOFFFEEDBACK)
24     )
25   {
26     MessageBox(NULL, "found debugger!", NULL, 0);
27   }
28   else
29   {
30     MessageBox(NULL, "no found debugger!", NULL, 0);
31   }
32
33   return 0;
34 }
```

自己在VC里实验了一下，果然能用

于是忽然想到，把它放在DllMain里，如果检测到有调试信息就return FALSE，使得程序不能正常初始化。实验了一下，果然好使，代码就不往上贴了，复制一下就是。

想在汇编下实现同样的功能，但是出了点问题，水平太次了，这么简单的功能，调了一下午也没调出来

最后发邮件询问大神，大神直接问，如果对方附加，你怎么办？

顿时心里凉了一截……

就是啊，人家等你启动后用OD附加，那就真的没办法了。唉，不灰心，权当玩了吧，至少也是一个思路不是~

另外，汇编写的程序真不知道怎么调试。放IDA里一点毛病也没发现，放OD里结果是出现了不能处理的异常……

难道只能一遍一遍看源码么！！！

转载于:https://www.cnblogs.com/02xiaoma/archive/2012/07/13/2590227.html